Effective:
1 January 2024
Version 015

AUSTRALIAN PAYMENTS NETWORK LIMITED

ABN 12 055 136 519

A Company limited by Guarantee

Code Set

for

ISSUERS AND ACQUIRERS COMMUNITY FRAMEWORK

Volume 2
Issuers Code

Commenced 1 July 2015

Australian Payments Network Limited
Telephone: (02) 9216 4888

Code Set for

ISSUERS AND ACQUIRERS COMMUNITY FRAMEWORK

Volume 2
Issuers Code

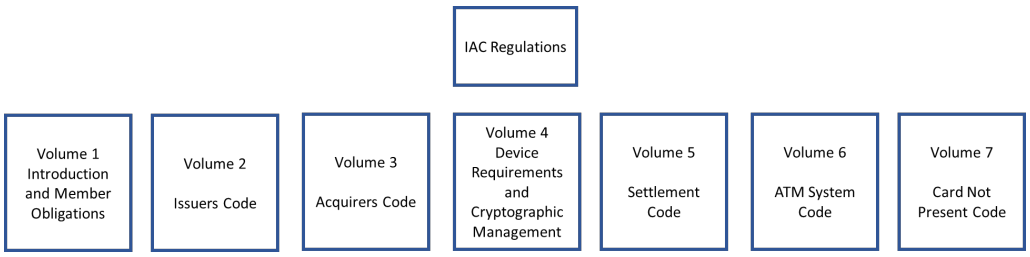
INDEX

PART 1 INTRODUCTIONINTERPRETATION AND DEFINITIONS

1.1 Purpose of this manual[1]

The IAC has been established to develop, implement and operate effective standards, policies and procedures to promote the efficiency, security and integrity of Australian Card Payments. These include minimum security standards, interoperability standards and value added services that support how payment cards are used throughout Australia.

These standards and requirements are contained within the IAC Code Set which is structured as follows:[2]



Volume 2 is intended for Issuers and contains, when read in conjunction with Volume 1, those aspects of Personal Identification Number (PIN) and device security that are considered mandatory for all Issuers participating within the IAC. In addition this volume contains guidance and recommendations into non-mandatory aspects of Issuer PIN management.

Part 2 of this volume identifies the mandatory standards specified by the IAC for PIN management as well as recommended practices for the handling of Cardholder PINs. Part 3 identifies minimum requirements and covers recommended practices for PIN change over open networks such as the Internet or mobile phones whilst Part 4 covers Device approvals and security. Part 5 of this volume, when read in conjunction with Volume 7, contains the requirements for Issuers dealing with Card Not Present Transactions, to mitigate the fraud associated with such Transactions. [3]

1.2 Interpretation

Interpretations are located in a separate document entitled ‘Interpretation & Definitions'.

1.3 Definitions

Definitions are located in a separate document entitled ‘Interpretation & Definitions’.

The next page is Part 2

[1] Amended effective 1/1/19, version 008 r&p 002.18
[2] Amended effective 1/7/19, version 009 r&p 001.19
[3] Amended effective 16/12/21, version 013 r&p 001.21

PART 2 ISSUER PIN MANAGEMENT AND SECURITY

2.1 PIN standards

Each Issuer must comply with the current version of ISO 9546.1 which specifies requirements for the management and security of any current PIN, to the maximum extent possible subject to their security policies and risk management requirements.[4]

2.2 Obligation to use compliant SCMs

SCMs used by Issuers for the handling or management of plaintext PINs and/or related keys must be approved for use by the Company in accordance with Part 3 of IAC Code Volume 4.[5]

2.3 Approval of new or modified SCMs

(a) Any Issuer certified in accordance with Part 3 of Volume 1 of the IAC Code ("certified Issuer"), who proposes to implement a new SCM, must apply for approval of the Device as required in accordance with clause 2.2.

(b) Any certified Issuer, which proposes to:

(i) implement any new SCM (not currently covered by an existing Letter of Approval);

(ii) continue to employ an SCM which has reached or is about to reach its 'Letter of Approval' sunset date, unless the Company has renewed the Device's Approval Period; or

(iii) implement any changes to an existing SCM's cryptographic devices, PIN or cryptographic key handling and management processing;

must apply for approval of the Device as required by clause 2.2 as if each Device is a new Device for the purposes of that section.

2.4 Cryptographic standards

Issuers must ensure that all cryptographic operations associated with the processing of Transactions and PIN management satisfy the cryptographic standards set out in IAC Code Set Volume 4 (Device Requirements and Cryptographic Management).

[4] Last amended 20/8/18, version 007 r&p 001.18
[5] Amended effective 16/12/21, version 013 r&p 001.21

2.5 PIN generation

Random, including customer-selected, PIN is the preferred option for PIN generation. Where a derived PIN is produced, the PIN derivation technique must be based on a cryptographic algorithm which employs a minimum key size of 128-bits.

2.6 PIN change

PIN change and PIN distribution over any form of open network (e.g., Internet, mobile phone) and not using SCDs, must conform to the minimum requirements specified in Part 3 clause 3.1 of this Volume 2, and have regard to the principles and best practice recommendations described in Part 3 of this Volume 2.[6]

2.7 Offline PIN

(a) If offline PIN verification is supported, Australian IC Cards that can be used to initiate a Transaction must be capable of Dynamic Data Authentication (DDA) or Combined Data Authentication (CDA).

(b) Protection of an offline PIN, during transmission to the IC Card must employ an asymmetric cipher mechanism compliant with part 7 of EMV 4.3 Specifications, Book 2 - Security and Key Management. The use of a separate PIN encryption key pair is highly recommended (available from www.emvco.org).

2.8 PIN block formats

Where a message contains PIN data, that PIN data must be formatted in accordance with one of the PIN block formats specified in ISO 9564.1, with the exception of formats 1 and 2.[7]

2.9 PIN entry attempts

The number of PIN entry attempts allowed by an Issuer to a Cardholder prior to disabling Card access is at the Issuer's discretion. However, it is recommended that the minimum number of PIN entry attempts (whether consecutive per an individual Transaction or cumulative over a given period of time – generally 24 hours) should be set at 3.

2.10 Transaction Verification[8]

(a) Issuers must ensure that for all Cards issued from 1 January 2026 all values for the variants of **Card Security Codes** are unique and unpredictable. This includes:

(i) the CVV2 (or equivalent CSC) printed on the card itself,

[6] Last amended effective 16/12/21, version 013 r&p 001.21
[7] Last amended effective 21/11/16, version 004 r&p 002.16
[8] Inserted effective 1/7/20, version 011 r&p 001.20

(ii) the CVC1 (or equivalent CSC) encoded in the magnetic stripe discretionary data, and

(iii) the iCCV (or equivalent CSC) encoded in the EMV Track Two Equivalent Data.

(b) The CVC1 and iCVV (or equivalent CSC) must be verified as correct for all transactions from 1 January 2026.

Next page is Part 3

PART 3 PIN USAGE OVER OPEN NETWORKS[9]

This Part 3 contains the principles and best practice recommendations as well as the minimum requirements for PIN usage in Issuer functionality offered over open networks which don't employ SCDs for PIN entry. This includes, but is not limited to, PIN change and delivery mechanisms, internet banking registration systems, and other internet product offerings by an Issuer. (See also clause 2.6 of this Volume 2).[10]

Where the new PIN is derived or generated by the Issuer (Issuer assigned PIN), delivery to the Cardholder is supported using Internet based mechanisms (e.g., browser based PC or smartphone) or using SMS messaging based mechanisms.

Where the new PIN is to be provided by the Cardholder (customer select PIN), only Internet based mechanisms are supported.

3.1 Minimum Requirements for Open Network PIN and PAN Functions[11]

Where an Issuer chooses to implement functionality, which involves open network transmission of the PIN, and where the principles and recommendations set out in clause 3.7 cannot be met, then:

(a) the requirements set out below must be followed:

(i) Concurrent existence of clear text PIN and PAN must be kept to the absolute minimum possible consistent with the functionality being implemented.

(ii) Identification of the Cardholder must use additional identifying data other than that contained on or in the Card itself.

(iii) Issuers must provide Cardholders with a means to determine that the dialogue with the Issuer is genuine.

(iv) Issuers must use calling-line identification only as a confirmation, not proof, of a Cardholder's identity, and must implement additional Cardholder authentication. *Note: authentication via a mobile app on the phone and the phone itself are considered as different verification methods.*

(v) All systems transporting PIN data or PAN data, or both, over open networks must provide mutual assurance to the Issuer and Cardholder that they are both genuine e.g. using a separate channel to deliver acknowledgements. *Note: messaging via a mobile app on the phone and the phone itself are considered as different channels.*

(vi) All events involving the PIN or PAN, or both, back to the Cardholder must be acknowledged using an out-of-band mechanism i.e. through the use of two separate channels working simultaneously to

[9] Amended effective 29/4/16, version 003 r&p 001.16

[10] Last amended effective 16/12/21, version 013 r&p 001.21

[11] Inserted effective 20/8/18, version 007 r&p 001.18

authenticate a Cardholder. *Note: messaging via a mobile app on the phone and the phone itself are considered as different channels.*

(vii) Issues must provide Cardholders with the means to confirm the outcome of events involving a PIN or a PAN or both.

(viii) Issuers must consider threats arising through device convergence resulting from technological change in selecting acceptable out-of-band mechanisms e.g. browser capable smartphones; and

(b) It is also strongly recommended that:

(i) The PIN should be encrypted immediately at the earliest point possible using an Issuer approved device.

(ii) Identification of the Cardholder should occur prior to the entry of the PIN.

3.2 Recommendations for PIN and PAN registration systems over open networks[12]

3.2.1 *Preferred model* [13]

Open network PIN and PAN registration systems leverage a customer's PAN and associated PIN for one time user identification and authentication credentials. The following principles should be applied to any PIN and PAN customer registration system over open networks (e.g., Internet, mobile phone etc.):

(a) The PIN and PAN customer registration system for internet banking should protect the PIN at all times it traverses the Issuer's system through strong encryption[14]. The PIN should be passed as an approved encrypted ISO format PIN block, either format 0 or 3, with format 3 preferred.

(b) Each PIN should be encrypted on the Cardholder's device to produce unique cipher text, (except by chance) to avoid the possibility of the construction of a rainbow[15] table.

(c) Except for on the Cardholder's device all decryption, translation, and re-encryption of PINs should occur within an approved SCM/HSM.

(d) The Cardholder's device should protect the PIN by forming an approved encrypted ISO format PIN block, either format 0, 3 or 4 immediately after PIN entry.

[12] Amended effective 20/8/18, version 007 r&p 001.18
[13] Inserted effective 20/8/18, version 007 r&p 001.18
[14] E.g. TDEA (112 bits of security), AES (128 bits and higher), RSA (2048 bits and higher), ECC (160 bits and higher), and ElGamal (2048 bits and higher). See NIST Special Publication 800-57 Part 1 (http://csrc.nist.gov/publications/) for guidance on cryptographic key strengths and algorithms.
[15] A rainbow table is a pre-computed table for reversing cryptographic hash functions, usually for cracking password hashes.

(e) The registration system should re-encrypt the customer's PIN block with a different PIN encrypting key as soon as it is received from the customer.[16]

In summary these principles are illustrated below.

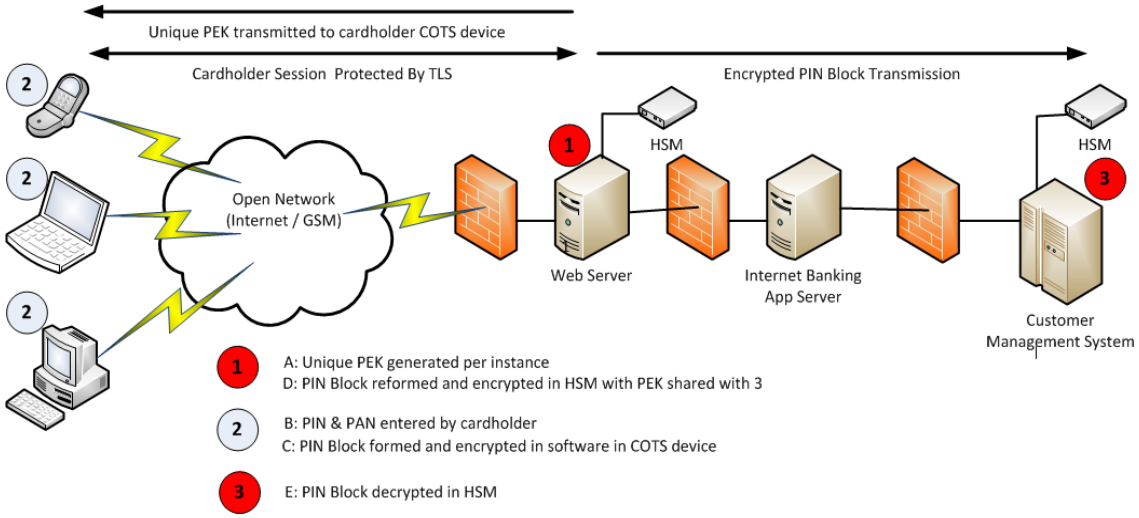


Figure 3.2. 1 – PIN encryption points during PIN and PAN Internet banking registration. (Example Architecture)

3.2.2 *Risk and security*[17]

Customer PIN and PAN registration should only be performed using an Issuer approved device (see clause 3.6) and functionality, and should follow the recommendations set out below:[18]

(a) PIN usage should adhere to the principles set out in ISO 9564 (all parts) to the maximum extent possible consistent with the Issuer's security and risk management policies;[19]

(b) the plain text PIN should never be transmitted over communications lines outside of a secure environment as specified in AS 2805.14.2:2009, clause H.5;

(c) PIN and PAN registration should ensure that the plain text PIN is never known to, or accessible by, any employee or agent of the Issuer;[20]

(d) a detailed risk assessment paying particular attention to any deviations from the relevant standards – [AS 2805.14, ISO 9564, ISO 13491] - should be an integral part of any Issuer's decision to provide functionality in support of PIN and PAN registration over open networks; and[21]

[16] Amended effective 20/8/18, version 007 r&p 001.18
[17] Amended effective 20/8/18, version 007 r&p 001.18
[18] Amended effective 20/8/18, version 007 r&p 001.18
[19] Amended effective 21/11/16, version 004 r&p 002.16
[20] Amended effective 20/8/18, version 007 r&p 001.18
[21] Amended effective 21/11/16, version 004 r&p 002.16

(e) to assist with fraud monitoring and problem resolution, Issuers should record PIN and PAN registration events including date, time, frequency and the channel over which the event occurred (without recording any PINs).

3.2.3 *Cardholder authentication* [22]

Issuers should:

(a) provide Cardholders with a means to determine that the dialogue with the Issuer is genuine;

(b) use calling-line identification only as a confirmation, not proof, of a Cardholder's identity, and to implement additional Cardholder authentication;

(c) ensure that PIN and PAN registration systems over open networks provide mutual assurance to the Issuer and Cardholder that they are both genuine e.g., using a separate channel to deliver acknowledgements;

(d) acknowledge PIN and PAN registration events back to the Cardholder using an out-of-band mechanism i.e., through the use of two separate networks working simultaneously to authenticate a Cardholder;

(e) pay particular attention to device convergence resulting from technological change in selecting acceptable out-of-band mechanisms e.g., browser capable smartphones; and

(f) provide Cardholders with the means to confirm the outcome of a PIN and PAN registration event.

3.3 Recommendations for PIN change and delivery over open networks [23]

3.3.1 *Preferred model* [24]

The following principles should be applied to any PIN change and delivery system over open networks (e.g., Internet, mobile phone etc.):

(a) The PIN change and delivery system should be separate to all other PIN processing and card management systems. Its domain should contain no Cardholder identifying/authentication information other than that associated with the PIN change and delivery system itself;

(b) The identification and authentication credentials for the PIN change and delivery system should be communicated to the Cardholder using a totally separate out-of-band channel [25] from that used by the Cardholder to initiate

[22] Amended effective 20/8/18, version 007 r&p 001.18
[23] Last amended effective 20/8/18, version 007 r&p 001.18
[24] Last amended effective 20/8/18, version 007 r&p 001.18
[25] Out-of-band authentication requires a separate, discrete pathway, such as a telecommunications network, be used in the authentication process. This provides a second secure channel in the event the primary Internet channel is compromised. An attacker would have to exploit both the Internet channel and the secondary one -- the phone network or end-user device -- to launch a successful attack.

the PIN change or issuance function. These credentials should be time bound and unique per PIN change or delivery event.

In summary these principles are illustrated below.

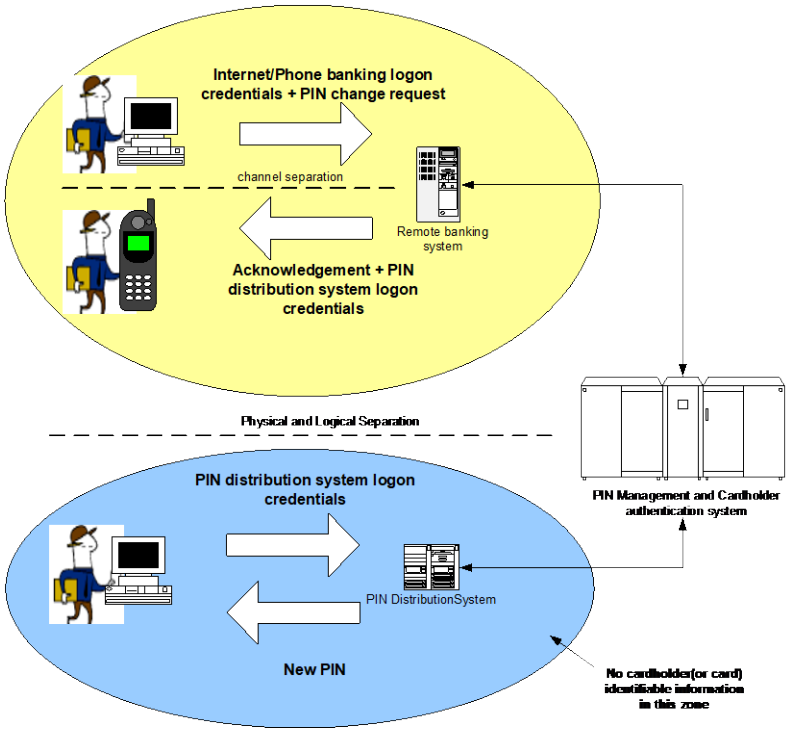


Figure 3.3.1A - Preferred model for Issuer assigned PIN issuance/change

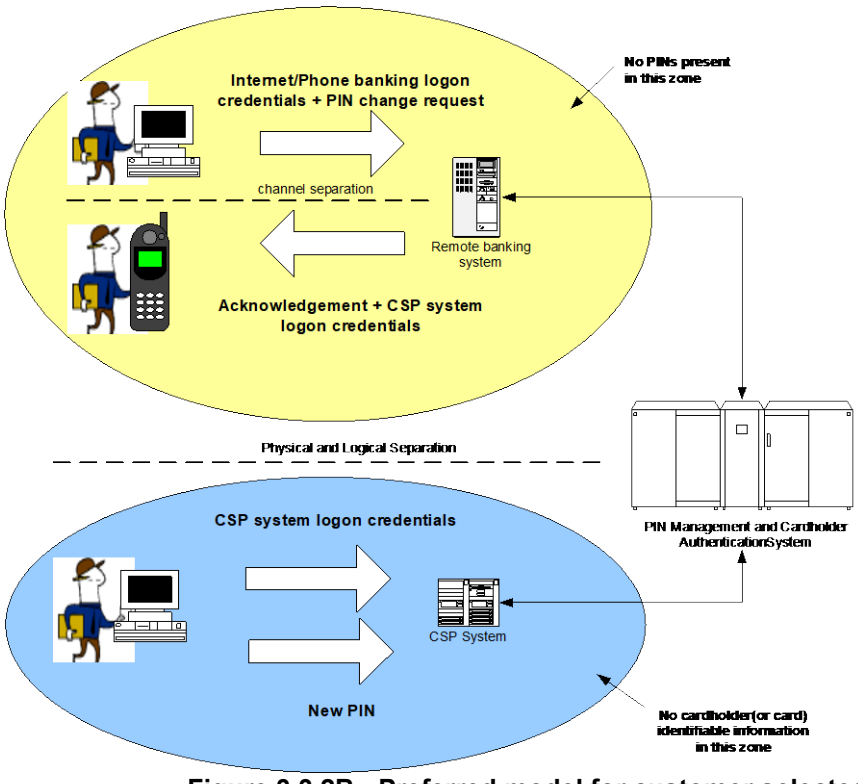


Figure 3.3.2B - Preferred model for customer selected PIN change

3.3.2 *Risk and security*[26]

Cardholder PIN change and delivery should only be performed using an Issuer approved device (see clause 3.6) and functionality, and should follow the recommendations set out below:[27]

(a) PIN change and delivery should adhere to the principles set out in ISO 9564 (all parts) to the maximum extent possible consistent with the Issuer's security and risk management policies;[28]

(b) PIN selection should not be performed using mail (traditional post or otherwise), unless specifically authorised in the IAC Code Set;[29]

(c) PIN change and delivery should ensure that the plain text PIN is never be known to, or accessible by, any employee or agent of the Issuer;[30]

(d) PIN change and delivery should only be initiated by the Cardholder;

(e) the host SCM functionality that is used to implement customer select PIN change should be atomic, that is, verification of the Cardholder using the current PIN or account specific control number should be an intrinsic part of that functionality. Specifically, an SCM function that accepts a new PIN and a PAN and that outputs an offset and/or PVV for storage in a host database should not exist unless it additionally embodies strong Cardholder authentication as per clause3.3.3;

(f) the PIN change and delivery process should ensure the authenticity of the Cardholder;[31]

(g) a detailed risk assessment paying particular attention to any deviations from the relevant standards – [AS2805.14, ISO 9564, ISO 13491] - should be an integral part of any Issuer's decision to provide functionality in support of PIN change and delivery over open networks; [32]

(h) to assist with fraud monitoring and problem resolution, Issuers should record PIN change and delivery events including date, time, frequency and the channel over which the event occurred (without recording any PINs); and[33]

(i) the Open Network PIN change/delivery system should not be the sole PIN change or delivery mechanism available to Cardholders.

[26] Last amended effective 20/8/18, version 007 r&p 001.18
[27] Last amended effective 20/8/18, version 007 r&p 001.18
[28] Amended effective 21/11/16, version 004 r&p 002.16
[29] Amended effective 29/4/16, version 003 r&p 001.16
[30] Amended effective 20/8/18, version 007 r&p 001.18
[31] Amended effective 29/4/16, version 003 r&p 001.16
[32] Last amended effective 21/11/16, version 004 r&p 002.16
[33] Amended effective 29/4/16, version 003 r&p 001.16

3.3.3 *Cardholder authentication* [34]

Issuers should:[35]

(a) provide Cardholders with a means to determine that the dialogue with the Issuer is genuine;

(b) ensure that Cardholder authentication credentials are not based on information that is publicly available;

(c) ensure that the Cardholder's card number cannot be determined solely from the Cardholder's authentication credentials;

(d) ensure that it is not possible to authenticate a Cardholder using only information contained on the card or other payment instrument;

(e) not transmit the PAN to the Cardholder during a PIN change or delivery operation, nor require that the Cardholder enter such information;

(f) implement a policy to never send unsolicited PIN change requests and advise Cardholders accordingly;

(g) use calling-line identification only as a confirmation, not proof, of a Cardholder's identity, and to implement additional Cardholder authentication;

(h) ensure that PIN change or delivery systems requiring the transmission of the PIN over open networks provide mutual assurance to the Issuer and Cardholder that the correct PIN is being delivered to, or from, the genuine Cardholder e.g., using a separate channel to deliver acknowledgements;

(i) avoid the use of the card PIN for non-payment transactions including access to electronic banking;[36]

(j) acknowledge PIN change and delivery requests back to the Cardholder using an out-of-band mechanism i.e., through the use of two separate networks working simultaneously to authenticate a user;

(k) pay particular attention to device convergence resulting from technological change in selecting acceptable out-of-band mechanisms e.g., browser capable smartphones;

(l) manage the risks associated with possible redirection of PIN change request or delivery acknowledgements through, for example, phone number porting;

(m) provide Cardholders with the means to audit the outcome of a PIN change or delivery request; and

[34] Amended effective 20/8/18, version 007 r&p 001.18
[35] Amended effective 29/4/16, version 003 r&p 001.16
[36] Amended effective 29/4/16, version 003 r&p 001.16

(n) ensure that no staff member can legitimately associate a control number with a card number or account.

3.4 Recommendations for PIN advice (assigned or derived PIN) over open networks[37]

3.4.1 *Methods of conveying the PIN [38]*

Issuer approved methods of conveying the PIN to the Cardholder should follow the recommendations set out below:[39]

(a) the plain text PIN should never be transmitted over communications lines outside of a secure environment as specified in AS 2805.14.2:2009, clause H.5, unless there is no feasible way in which the PIN could be associated with the Cardholder, the Cardholder's account or card;

(b) the Issuer's employees, staff and agents should not handle the plain text PIN where any of the associated card or account details are also available to them;

(c) Issuers should appropriately evaluate and manage the risks associated with change of destination requests from Cardholders;

(d) Issuers should examine, on a regular and frequent basis, their procedures and associated risks for delivering cards and PINs to Cardholders.

(e) Issuers should ensure that physical distribution of a PIN is made only to pre-registered Cardholder destinations;[40]

(f) Issuers should ensure that electronic distribution of a PIN is made only to strongly authenticated Cardholders as per clause 3.3.3.[41]

3.4.2 *PIN advice by SMS (Issuer assigned PIN)*

In addition to the recommendations set out in clause 3.4.1, where an Issuer assigned PIN is conveyed to the Cardholder via an SMS message, the recommendations set out below should be followed: [42]

(a) Issuers should provide the Cardholder with security advice for the management of the mobile phone used for PIN advice. This should include advice about the dangers of malware and of storing account data or PINs, or both, on the phone or any additional copies made of the phone data e.g., via synchronizing the data between the mobile phone and a personal computer;[43]

[37] Amended effective 20/8/18, version 007 r&p 001.18
[38] Inserted effective 20/8/18, version 007 r&p 001.18
[39] Last amended effective 20/8/18, version 007 r&p 001.18
[40] Amended effective 20/8/18, version 007 r&p 001.18
[41] Amended effective 20/8/18, version 007 r&p 001.18
[42] Last amended effective 20/8/18, version 007 r&p 001.18
[43] Amended effective 20/8/18, version 007 r&p 001.18

(b) only pre-registered mobile phone numbers should be used for PIN advice;

(c) if control numbers and authentication values are used then the SMS PIN advice message should be preceded by a communication to the Cardholder containing an identification value or control number and an authentication value. This communication should use a different mechanism other than SMS;

(d) the identification value or control number and authentication values should not disclose the account or card numbers;

(e) if the identification value is publicly available, such as the Cardholder's phone number or email address, then a second non-public identification value or mechanism should be used;

(f) the PIN distribution system should have no way of associating an identification value with a specific Cardholder's name, address, account or card number;

(g) all PINs, control values and authentication data should be encrypted using strong encryption[44] during transmission to, and storage in, the PIN distribution and PIN management systems;

(h) the PIN advice message should be preceded by a Cardholder initiated request;

(i) the PIN request message should contain the Cardholder's identification and authentication values;

(j) the PIN distribution system should transmit the PIN to the Cardholder only upon successful validation of the authentication value;

(k) the PIN distribution system should have limits on the number of attempts made to retrieve a PIN;

(l) it should not be possible for authorised staff with access to the PIN distribution system to access any other system where associated Cardholder data can be accessed. Additionally the PIN distribution system database should be separate to any other database containing Cardholder data;

(m) the authentication and identification values together with the PIN should be deleted from the PIN distribution system immediately after successful delivery is confirmed;

(n) the Issuer should establish an allowable storage window for the PIN distribution system after which time the PIN should be deleted from the system whether delivered or not;

(o) the PIN distribution system should run on a dedicated system and be isolated from any other network by a dedicated firewall;

[44] See 3.1 (a)

(p) the PIN distribution system should perform no other function than PIN distribution and any sessions established during the distribution should be terminated once the PIN has been sent;

(q) the association of the PIN to a specific account or card number should not be possible with the authorising information available on the PIN distribution system;

(r) where required, the PIN distribution system should decrypt the PIN immediately prior to transmission to the Cardholder;

(s) it should not be possible to identify the type of Cardholder payment device, account or card number from the SMS message containing the PIN.

3.4.3 *PIN advice by internet (Issuer assigned PIN)*

In addition to the recommendations set out in clause 3.4.1, the recommendations set out below should be followed where the PIN is communicated to the Cardholder using the internet:[45]

(a) Issuers should provide the Cardholder with security advice for the management of the end-user device (e.g., PC, Smartphone, etc.) used for PIN advice. This should include advice about the dangers of malware and of storing account data e.g., Cardholder statements and/or PINs on the end-user device or any additional copies made of the data e.g., backups;

(b) the PIN should be cryptographically protected whilst in storage or transmission using strong encryption[46]. PIN transmission should be in accordance with the recommendations in clause 3.7 ;[47]

(c) the encrypted PIN should be decrypted for display on the end-user device's display by the Issuer-provided application;

(d) initiation of the PIN advice should require that the Cardholder enter pre-established credentials such as a control number and authentication value;

(e) as the security of the PIN advice implementation is based on the premise that no individual, other than the Cardholder, can associate the control number with a specific account or card number, it is essential that the pre-established credentials should not disclose the card or account numbers;

(f) if control numbers and authentication values are used then the control number and authentication values should be communicated using an out-of-band mechanism i.e., through the use of two separate networks working simultaneously to authenticate a user;

(g) any key used to generate a control number should not be used for any other purpose and shall be managed in accordance with AS 2805.6.1;

[45] Last amended effective 20/8/18, version 007 r&p 001.18
[46] See 3.1(a)
[47] Amended effective 20/8/18, version 007 r&p 001.18

(h) the PIN, and if control numbers and authentication values are used, then the authentication values as well, should not be logged and should be deleted immediately after use;

(i) if control numbers and authentication values are used then issuers should ensure that the association of Cardholder authentication credentials with a control number does not weaken the principle that the control number cannot be used to determine a specific account or card number;

(j) if control numbers and authentication are used then Cardholder authentication should not be performed by the Internet server but rather by the back end Issuer host system and only after the control number has been re-associated with a specific account;

(k) web servers should be configured to disable client side caching of web pages that display PIN and associated data during the Internet session.

(l) if control numbers and authentication values are used then the control number should be generated and delivered to the Cardholder in such a way, e.g., by using a tamper evident mailer, such that no-one, other than Cardholder, can associate that control number with that Cardholder without detection;

(m) if control numbers and authentication values are used then the control number should be communicated to the Cardholder in such a way that no-one, other than the Cardholder, can access it without detection;

(n) if control numbers and authentication values are used then the PIN distribution system should have no way of associating a control number with a specific Cardholder's name, address, account, card or phone numbers;

(o) if control numbers and authentication values are used then the PIN advice function should exchange only strings of numbers (a control number and authentication values) with the Issuer PIN distribution system i.e., there should be no other Cardholder identifying information, other than the control number, exchanged during the PIN delivery function;

(p) if control numbers and authentication values are used then the PIN management system should re-associate the control number with a specific account number, validate the Cardholder using the authentication values and retrieve the Cardholder PIN for that account number;

(q) if control numbers and authentication values are used then the PIN distribution system should be designed and operated under strictly enforced conditions such that no individual, other than the Cardholder, is able to associate a control number, PIN or authentication values with any specific card or account number;

(r) if control numbers and authentication values are used then PIN delivery to the end-user equipment (e.g., PC or smart-phone) should not be associated with any Cardholder account data or card number;

(s) internet PIN advice should be protected using a secure channel established between the client application and the PIN distribution system according to the principles set out in ISO/IEC 11770; and

(t) the implementation should take into account malware attacks such as man-in-the-browser or man-in-the-middle.

3.5 Recommendations for Customer select PIN change over open networks[48]

3.5.1 *Issuer's actions*[49]

Issuers should: [50]

(a) advise Cardholders against using the PIN as a credential for electronic banking or any other service and provide an alternative input format for electronic banking credentials e.g., forbidding all numeric passwords;[51]

(b) provide the Cardholder with appropriate guidance for PIN selection and usage; and

(c) provide and use cryptographic mechanisms for protecting the PIN from the point of entry and beyond.

3.5.2 *Customer select PIN change by Internet*

In addition to the recommendations in clause 3.5.1, Issuers should follow the recommendations set out below where the Cardholder is allowed to change the PIN using the internet:[52]

(a) Issuers should provide the Cardholder with security advice for the management of the end-user device used for PIN selection. This should include advice about the dangers of malware and of storing account data and/or PINs on the end-user device or any additional copies made of the device's data e.g., backups;

(b) the PIN should be cryptographically protected whilst in storage or transmission using strong encryption[53]. PIN transmission should be in accordance with the recommendations in clause 3.7;[54]

(c) initiation of PIN selection should require that the Cardholder enter pre-established credentials such as a control number and authentication value;

(d) as the security of the PIN selection is based on the premise that the design and implementation of the system is such that no individual, other than the Cardholder, can associate the control number with a specific account or

[48] Amended effective 20/8/18, version 007 r&p 001.18
[49] Inserted effective 20/8/18, version 007 r&p 001.18
[50] Inserted effective 20/8/18, version 007 r&p 001.18
[51] Amended effective 20/8/18, version 007 r&p 001.18
[52] Last amended effective 20/8/18, version 007 r&p 001.18
[53] See 3.1(a)
[54] Amended effective 20/8/18, version 007 r&p 001.18

card number it is essential that the control number and authentication value, where used, not disclose the card or account numbers;

(e) If control numbers are used then the control number and authentication values should be communicated using an out-of-band mechanism i.e., through the use of two separate networks working simultaneously to authenticate a user;

(f) any key used to generate a control number should not be used for any other purpose and should be managed in accordance with AS 2805.6.1;

(g) the PIN and authentication values should not be logged and must be deleted immediately after use;

(h) internet PIN selection should be protected using a secure channel established between the client application and the CSP PIN management system according to the principles set out in ISO/IEC 11770;

(i) the implementation should take into account malware attacks such as man-in-the-browser or man-in-the-middle;

(j) Issuers should ensure that the association of Cardholder authentication credentials with a control number does not weaken the principle that the control number cannot be used to determine a specific account or card number;

(k) if control numbers are used then Cardholder authentication should not be performed by the Internet server but rather by the back end Issuer host system and only after the control number has been re-associated with a specific account;

(l) web servers should be configured to disable client side caching of web pages that display PIN and associated data during the Internet session.

(m) If control numbers are used then the control number should be generated and delivered to the Cardholder in such a way (e.g., by using a PIN mailer) that no-one, other than Cardholder, can associate that control number with that Cardholder without detection;[55]

(n) the control number should be communicated to the Cardholder in such a way that no-one, other than the Cardholder, can access it without detection;

(o) the CSP PIN change system should have no way of associating a control number with a specific Cardholder's name, address, account, card or phone number;

(p) the PIN advice function should exchange only strings of numbers (a control number and authentication values) with the Issuer CSP PIN change system i.e., there should be no other Cardholder identifying information, other than the control number, exchanged during the PIN change function;

[55] Amended effective 29/4/16, version 003 r&p 001.16

(q) the PIN management system should re-associate the control number with a specific account number, validate the Cardholder using the authentication values and retrieve the Cardholder PIN for that account number;

(r) the CSP PIN change system should be designed and operated under strictly enforced conditions such that no individual is able to associate a control number, PIN or authentication values with any specific card or account number;

(s) Cardholder authentication and generation of the reference PIN should be done in real-time during the session with success or failure reported back to the Cardholder.

3.5.3 *Customer select PIN Change by mobile phone*

(a) PIN selection via SMS or DTMF tone signalling should not be permitted.[56]

(b) The use of Internet-based PIN change on Internet-enabled mobile phones should follow the recommendations of clause 3.5.2.[57]

3.6 Recommendations for Issuer approved Devices used to enter PINs[58]

3.6.1 *Device Guidelines[59]*

In accordance with clause 3.3.2, only Issuer approved devices should be used for PIN entry supporting PIN change or selection or PIN and PAN registration. Such devices should be one or more of the following: [60]

(a) a functionally secure device i.e., a device that can be compromised only by physical means and whose functionality cannot be subverted through unauthorised inputs to the device (refer to ISO 9564.4); or[61]

(b) a device providing a level of logical security sufficient to protect the PIN and other account data.

3.6.2 *Issuer's actions[62]*

Issuers should ensure that:[63]

(a) Cardholders are fully educated as to their responsibilities for the management and protection of permitted personal devices;

(b) Cardholders are adequately warned about the inherent dangers in storing the PIN;

[56] Amended effective 20/8/18, version 007 r&p 001.18
[57] Last amended effective 20/8/18, version 007 r&p 001.18
[58] Amended effective 20/8/18, version 007 r&p 001.18
[59] Inserted effective 20/8/18, version 007 r&p 001.18
[60] Amended effective 29/4/16, version 003 r&p 001.16
[61] Amended effective 20/8/18, version 007 r&p 001.18
[62] Inserted effective 20/8/18, version 007 r&p 001.18
[63] Amended effective 29/4/16, version 003 r&p 001.16

(c) Cardholders are provided with a means of ensuring that the communication is genuinely with the Issuer;

(d) it is possible for the Cardholder to determine that a genuine end-to-end communication with the Issuer is occurring rather than a phishing or other man-in-the-middle malware masquerading as the Issuer application;

(e) the PIN is protected with strong encryption[64] between the approved personal use device and the Issuer;[65]

(f) Cardholders are provided with easy access to applicable malware countermeasures for any approved personal use devices and be made aware of the risks associated with malware;

(g) PIN change, and PIN and PAN registration applications should provide a mechanism to protect the PIN during PIN entry in case man-in-the-browser or other root-kit attacks are in place, that are undetectable by common anti-virus countermeasures.[66]

3.7 Recommendations for PIN transmission[67]

3.7.1 *PIN protection* [68]

PINs and associated account data transmitted between systems should be protected against disclosure, and the integrity of the PIN protected against any party eavesdropping on, or manipulating, the communications link. PIN integrity refers to the integrity of the relationship between the PIN and any associated information such as user account data.[69]

3.7.2 *Issuer's actions* [70]

Issuers should:[71]

(a) protect the PIN during transmission by at least one of the following methods;

(i) provision of physical protection;

(ii) encryption of the PIN value; or

(iii) disassociation of the PIN from the account data, with PIN integrity maintained through the use of an encrypted control value;

[64] See 3.1(a)
[65] Amended effective 29/4/16, version 003 r&p 001.16
[66] Amended effective 29/4/16, version 003 r&p 001.16
[67] Amended effective 20/8/18, version 007 r&p 001.18
[68] Inserted effective 20/8/18, version 007 r&p 001.18
[69] Amended effective 29/4/16, version 003 r&p 001.16
[70] Inserted effective 20/8/18, version 007 r&p 001.18
[71] Amended effective 29/4/16, version 003 r&p 001.16

(b) use transmission protocols designed such that the introduction of fraudulent messages, or modification of valid messages, does not yield any useful information concerning the PIN;

(c) use cryptographic mechanisms such that PIN integrity is ensured;

(d) where the PAN is available, only encipher PINs using one of the PIN block formats specified in ISO 9564.1 with format 3 preferred; [72]

(e) where the PAN is not available;

(i) use an encrypted control value uniquely linked to the PAN to construct the PIN block. The construction should provide the same security properties as provided by ISO PIN blocks;

(ii) the method used to format the PIN block prior to encryption should not enable the PIN to be recovered from the resulting ciphertext (e.g., by using rainbow tables[73]);

(f) ensure that any PIN translation conforms to the guidance in ISO 9564.1, but only to the extent that such guidance is consistent with the Issuer's security and risk management policies;

(g) If control numbers are used then ensure that the association of Cardholder authentication credentials with the control number does not weaken the principle that the control number cannot be used to determine a specific account;[74]

(h) use only cryptographic algorithms specified in ISO 9564.2 to provide PIN secrecy and integrity; and[75]

(i) ensure that clear text PIN transmission does not contain any information that can be directly connected with the Cardholder or the account/card number.

Next page is Part 4

[72] Last amended effective 21/11/16, version 004 r&p 002.16
[73] See 3.1(b)
[74] Amended effective 29/4/16, version 003 r&p 001.16
[75] Amended effective 29/4/16, version 003 r&p 001.16

PART 4 DEVICE SECURITY STANDARDS

This Part 4 sets out the minimum security standards applicable to Secure Cryptographic Devices (SCDs), including HSMs/SCMs and Key Loading devices (KLDs) that are required to be met by all Issuers.

4.1 Relevant standards [Deleted][76]

4.2 Secure Cryptographic Devices

(a) All Devices involved in the production, distribution, selection, entering and transmission of plaintext Cardholder PINs, or associated cryptographic keys used to protect Cardholder PINs in the Interchange environment must be approved for use using the process described in IAC Code Set Volume 4 (Device Requirements and Cryptographic Management).

(b) If an Issuer wishes to implement a new SCD for which a Letter of Approval is not held, the Issuer must arrange for that device to be approved in accordance with the Device Approval Process.[77]

4.3 Device management

4.3.1 *Security Control Modules (Host Security Modules)* [78]

(a) SCMs shall be managed in accordance with the requirements of AS 2805.14.2. The Sponsor must submit to the committee of management an annual compliance statement confirming compliance with Annexures A.3, C.3, E.3 of this Volume 2 and either H.4 or H.5 of AS 2805.14.2 (in respect of any SCMs employed in the implementation of Interchange Transactions. Annexure B.3 of Volume 1 used in connection with the Annual Security Audit (see IAC Code Set Volume 1 (Introduction and Member Obligations), provides the required confirmation.

4.3.2 *Key Loading and Transfer Devices (KLDs, KTDs)*

Devices used in the initial cryptographic key loading of SCMs or PEDs must be managed in accordance with the requirements of AS 2805.14.2. The Sponsor must submit to the committee of management an annual compliance statement confirming compliance with Annexes A.3, E.3 and F.3 of AS 2805.14.2 in respect of any devices employed in the initial loading and transfer of SCM or PED cryptographic keys (see Annexure B.3 of Volume 1 (Introduction and Member Obligations used in conjunction with the annual Security Audit programme (see IAC Code Set Volume 1 (Introduction and Member Obligations)), provides the required confirmation.

[76] Deleted effective 16/12/21, version 013 r&p 001.21
[77] Amended effective 16/12/21, version 013 r&p 001.21
[78] Amended effective 16/12/21, version 013 r&p 001.21

4.4 Security Control Module - limitations on functions [Deleted][79]

4.5 Remote management of Security Control Modules

This clause applies to systems which support remote access for the management of SCMs.

4.5.1 *SCM access requirements*

(a) SCMs must be located in a secure, protected network, separate from generic internal or external access;

(b) there must not be uncontrolled connections between general internal and external networks;

(c) SCMs must be accessible only to authorised hosts and authorised applications;

(d) for TCP/IP implementations:

(i) the SCM environment must be protected at a minimum by an IPS or IDS between the perimeter network firewall and the remote management device;

(ii) stateful firewalls must protect all external entry points to the SCM environment;

(iii) such firewalls must log and monitor all inbound and outbound traffic to the SCMs.

(e) there must be a procedure, which is audited on a regular basis, for the rapid disablement of known/suspected compromised remote management devices.

4.5.2 *Management of SCM Remote Management Solutions*

(a) Remote Management Solutions ("RMS") may only be used with AusPayNet approved SCMs;

(b) all SCM RMS must have been approved in accordance with the Device Approvals Process;[80]

(c) remote management devices may only be deployed in a minimally controlled environment, a controlled environment or a secure environment as per Annex H of AS 2805.14.2. At a minimum:

(i) the storage of the RMS must be under dual control;

[79] Deleted effective 16/12/21, version 013 r&p 001.21
[80] Amended effective 16/12/21, version 013 r&p 001.21

(ii) the operation of the RMS must be under dual control; and

(iii) while the RMS is in operation access must be restricted to authorised personnel.

Next page is Part 5

PART 5 CARD NOT PRESENT TRANSACTIONS[81]

5.1 Compliance Provision

Each Issuer must comply with the obligations in Part 3 clause 3.1 of the IAC Code Set Volume 7 (Card Not Present Code).

Next page is Annexure A

[81] Amended effective 1/1/20, version 010 r&p 002.19

Annexure A GUIDELINES FOR ISSUING PREPAID CARDS

[Informative]

This annexure provides guidelines for IA Participants which participate or propose to participate in the issuance and/or acceptance of Prepaid Cards.

A.1 CARD CHARACTERISTICS

Prepaid Program Providers and sponsoring Issuers should ensure that Prepaid Cards comply with the following guidelines:

(a) Card physical characteristics;

Prepaid Cards should as a minimum, meet the specifications detailed in AS 3521, 3522 and 3524. These standards contain requirements for physical characteristics, dimensions, layout of information and format for encoding Tracks 1 and 2 of the magnetic stripe.

(Note: Cards that do not comply with these guidelines may not be able to generate Transactions at ATMs and/or EFTPOS Terminals.)

(b) Minimum descriptive requirements for Prepaid Cards;

(i) Prepaid Cards may, on their front face;

(A) be clearly identified as a Prepaid Card; and

(B) clearly indicate that they should only be used when online authorisation is available (the words "Electronic use only" or similar are recommended);

(ii) The embossing of the PAN and expiry date on Prepaid Cards is optional.

(Note: Prepaid Program Providers and sponsoring Issuers should consider the requirements of other regulatory instruments such as the Australian Securities and Investment Commission's Regulatory Guide 185: Non-Cash Payment Facilities and as an example, its requirements in respect of expiry dates.)

A.2 ENCODING AND TRANSMISSION OF TRACK 2 DATA

(a) Prepaid Program Providers and sponsoring Issuers should ensure encoding of Track 2 on Prepaid Cards in accordance with the requirements of AS 3524 (encoding of Track 1 and Track 3 on Prepaid Cards is optional).

(b) Acquirers should transmit all Track 2 data received by the Acquirer from the Terminal to the Issuer without alteration.

A.3 PERSONALISATION

There are no mandatory requirements for the personalisation of Prepaid Cards.

A.4 SIGNATURE PANEL REQUIREMENTS

There is no mandatory requirement for a signature panel on Prepaid Cards.

A.5 PIN STANDARDS

(a) The use of a PIN for Cardholder authentication is not mandatory.

(b) However, when prompted for a PIN, the entry of at least a four digit number by the Cardholder is mandatory to facilitate the carriage of the Transaction across the Interchange network.

A.6 UNIQUE BINS

Prepaid Program Providers and sponsoring Issuers should ensure that Prepaid Cards are only issued under BINs that are unique from BINs under which non Prepaid Cards are issued.

A.7 TEST CARDS

Prepaid Program Providers and sponsoring Issuers that give notice of the introduction of a new BIN or a change to the routing of an existing BIN for a Prepaid Card pursuant to clause 2.8.2 in the IAC Code Set Volume 1 (Introduction and Member Obligations) must, on request by the affected IAC Members ensure production of any necessary test Cards in sufficient time to allow testing to occur before the applicable Institutional Identifier Change Date.

A.8 INTERCHANGE SETTLEMENT

Prepaid Card Transactions must be settled in accordance with IAC Code Set Volume 5 (Settlement Code).

A.9 DISPUTES

(a) Prepaid Cards are not generally issued with a secure owner authentication mechanism. Therefore, unless bilaterally agreed to the contrary:

(i) Prepaid Cardholder disputes are to be resolved by the applicable Prepaid Program Provider; and

(ii) the other parties involved in the Transaction should co-operate with the Prepaid Program Provider.

(b) It is recommended that IAC Members agree to apply standard IAC dispute resolution processes to Transactions initiated with Prepaid Cards if a PIN (the security of which is managed in accordance with Part 2 of this Volume 2) was issued to the original Prepaid Cardholder.

(c) Settlement disputes between IAC Members are to be resolved in accordance with IAC Code Set Volume 5 (Settlement Code).

Next page is Annexure B

Annexure B PIN CHANGE OVER OPEN NETWORKS – GUIDELINES [DELETED][82]

[Deleted]

Next page is Annexure C

[82] Deleted effective 20/8/18, version 007 r&p 001.18

Annexure C DEBIT CARD FRAUD PREVENTION GUIDELINES

[Informative]

Annexure C is confidential

[83] Amended effective 29/4/16, version 003 r&p 001.16

The next page is Annexure D

Annexure D THIRD PARTY DIGITAL WALLET SECURITY: CARD ISSUER GUIDELINES[84]

[Informative]

Best practice guidelines for Card Issuers in relation to third party mobile wallet security

D.1 CONTEXT

D.1.1 INTRODUCTION

AusPayNet is Australia's peak payments industry association. We work with our members and other payments industry stakeholders to identify and manage security risks in payment systems and payment technologies.

AusPayNet supports payments technology innovation that meets Australian security requirements and that preserves consumers' confidence and trust in the payments system. Mobile banking and payment services, mobile / digital wallets and third party digital wallets are emerging features of the global and Australian payments landscape that potentially offer significant consumer benefits.

Digital or mobile wallets are software applications on consumer devices which act as a repository for payment and other cards, and which by provisioning encrypted payment card data, effectively enable 'card present' mobile payment transactions at POS and in application. Third Party Digital Wallets are those which may be provided by a third party using multiple Card Issuers' payment Card data, customer relationships and existing payment networks, as well as various intermediaries and service providers. Australians are well-served by a robust consumer protection framework for mobile banking and mobile payment services - the *ePayments Code* – which attributes primary liability for unauthorised transactions made by use of such facilities to the Card Issuer subscriber which has promoted or endorsed that facility, even where the liability might be attributable to another party in the shared network.

These Guidelines have been issued by AusPayNet as *industry best-practice* to help Card Issuer members of the IAC to understand and proactively manage potential fraud and security risks in the provision of Third Party Digital Wallet services. They are voluntary.

As an adjunct to the Guidelines, AusPayNet will periodically convene open mobile payments industry fora, develop publications and white papers and invite consultation to promote understanding of, and consider developments in, mobile payments security and fraud management issues.

D.1.2 SCOPE

The Guidelines focus on the issues which typically require consideration by a Card Issuer in the context of provisioning its Cards to third party mobile wallets,

[84] Amended effective 21/11/16, version 004 r&p 002.16

including customer identification and verification, authentication of transactions and management of token generation and Card data security.

These Guidelines are not intended to address the issues of liability apportionment between Cardholders, Card Issuers, Digital Wallet Providers and other parties to a Third Party Digital Wallet transaction: this is a proprietary matter for parties to resolve.

The Guidelines do not apply to software applications that process payments solely using card-on-file data provided directly by a Cardholder to the payment service provider, where 'card-not-present' liability arrangements apply.

The Guidelines have not been drafted to apply to Card Issuers' proprietary mobile banking applications or proprietary wallet services, being those provided by a Card Issuer solely for its own customers. The responsibility for managing fraud and security of proprietary wallet services, and the liability for, and reputational risk associated with, losses resulting from use of proprietary products, rests entirely with the Card Issuer. A Card Issuer may choose to apply aspects of these Guidelines to its proprietary mobile banking applications and wallet services where appropriate.

D.1.3 OBJECTIVES

(a) The purpose of the Guidelines is to assist Card Issuers with establishing their respective security and data privacy requirements for Third Party Digital Wallets to promote the integrity and security of these services.

(b) The Guidelines are voluntary and are intended to represent industry best practice for security and tokenisation of mobile payment transactions and for privacy and limited permitted disclosure of Cardholder and mobile payments data.

(c) The Guidelines are not intended to, and do not, of themselves:

  (i) presume, affect or prescribe the terms of any arrangement established by any Card Issuer with any Digital Wallet Provider/s;

  (ii) affect the rights of any Card Scheme administrator to establish scheme rules for provisioning its co-branded Cards to Digital Wallets or the obligations of any Card Issuer under those rules;

  (iii) affect the right of any Card Issuer to exercise commercial freedom in the selection of mobile payments services processors and partners;

  (iv) affect the obligations of any Card Issuer as a subscriber to the ePayments Code or to its Cardholders more generally; or

  (v) affect the right of any Card Issuer to determine to apply different requirements and standards to those set out in the Guidelines.

(d) The Guidelines are technology neutral and are not to be construed as promoting, endorsing or impeding any particular service provider/s.

(e) Card Issuers are encouraged to promote awareness of the Guidelines amongst Digital Wallet Providers, Card Scheme administrators, and other participants in the provision of Digital Wallet services.

(f) Card Issuers are encouraged to ensure that the provisioning of Cards to a Third Party Digital Wallet does not affect or derogate from the intrinsic capabilities and functions of Cards, or any priority network arrangement that applies to them.

(g) AusPayNet does not monitor or enforce any Card Issuer's adoption or use of, or compliance with, these Guidelines.

(h) AusPayNet will periodically review these Guidelines to ensure they remain effective and relevant, particularly as international standards for mobile payments develop, and may amend them from time to time.

D.1.4 GLOSSARY

In this document:

AusPayNet means Australian Payments Network Limited (ABN 12 055 136 519).

BIN means the bank identification number allocated in accordance with ISO/IEC 7812.

Card means any card, device, application or identifier provided by an Issuer, which is linked to an account or credit facility with the Card Issuer.

Cardholder means a customer of an Issuer who is issued with a Card and PIN or other authentication method or process.

Card Issuer means a body corporate which, pursuant to the rules of a Card Scheme, issues a Card to a Cardholder and, in connection with any Card transaction effected using that Card assumes obligations to the relevant Cardholder, which obligations are in the first instance discharged on its behalf by an acquiring institution.

Card Scheme means the set of functions, procedures, arrangements and rules that enable a Cardholder to make payment transactions with a third party other than the Card Issuer. For the avoidance of doubt, a Card Scheme may be a three-party scheme or a four-party scheme.

CVM means Cardholder verification method.

Digital Wallet means a software application on a digital device that:

(a) functions as a digital container for payment Cards, tickets, loyalty cards, receipts, vouchers and other forms of payment; and

(b) provisions and uses the encrypted Card data associated with an enrolled payment Card.

For the avoidance of doubt, a software application that processes payments solely using 'card on file' data is not a Digital Wallet for the purposes of these Guidelines.

Digital Wallet Provider means a body corporate which is a third party provider of Digital Wallet services to its, and a Card Issuer's, mutual customers/Cardholders.

ePayments Code means the electronic payments code published by ASIC, as amended from time to time.

EMV Card means a Card issued by a Card Issuer that contains an integrated circuit that conforms to EMV specifications, in respect of which the EMV Issuer Country Code data element (tag 5F28) is equal to "036".

IAC means the Issuers and Acquirers Community constituted by the Regulations.

ID&V means identification and verification.

PAN means primary account number.

Privacy Act means the *Privacy Act 1988 (Cth).*

Regulations mean the regulations for the IAC, as prescribed by AusPayNet, as amended from time to time.

Third Party Digital Wallet means a Digital Wallet that is provided by a Digital Wallet Provider.

TSP means an entity that provides a token service, comprising a token vault and related processing, and which has the ability to use licensed ISO BINs as token BINs to issue payment tokens for PANs that are submitted in accordance with EMV Co's *Payment Tokenisation Specification*, version 1.0 (March 2014).

D.2 GUIDELINES

D.2.1 SECURITY

D.2.1.1 Customer identification and authentication on enrolment

(a) The Card Issuer is responsible for making the decision as to whether a particular Card can be enrolled in a Third Party Digital Wallet.

(b) The Card Issuer is responsible for determining appropriate ID&V methods and the data elements required to support enrolment of its Cards into Third Party Digital Wallets. In determining appropriate ID&V levels, the Card Issuer should have regard to the following criteria:

(i) Enrolment ID&V for Third Party Digital Wallets should achieve levels of security that are, as a minimum, equivalent to ID&V used in the Card Issuer's proprietary digital wallets and/or Card Issuer mobile banking applications;

(ii) any 3D Secure processing standards which may apply (if a Card-based ID&V process is to be used); and

(iii) any relevant global industry best practices for ID&V.

(c) The Card Issuer may outsource key parts of its ID&V process to a third party (including the Digital Wallet Provider), but should ensure the third party meets the requirements in this section 1.1.

(d) The Card Issuer may authorise the enrolment of a particular Card in more than one Third Party Digital Wallet.

D.2.1.2 Customer authentication at the time of transaction

(a) The Card Issuer is responsible for determining the appropriate CVM for authenticating transactions made using the Card Issuer's issued Cards in accordance with any relevant Card Scheme rules in place for those Cards. To the extent the Card Issuer has the right to exercise discretion when determining appropriate CVMs, the Card Issuer should do so having regard to the following criteria:

(i) CVM for transactions in Third Party Digital Wallets must achieve levels of security which are as a minimum equivalent to CVM for transactions made using EMV Cards;

(ii) industry best practice; and

(iii) any list of CVMs that may have been approved by AusPayNet for Card Payments in Australia.

(b) The Card Issuer should not use a CVM which is:

(i) inconsistent with the CVMs prescribed by the relevant Card Scheme rules applicable to the Card; or

(ii) not in AusPayNet's approved list of CVMs for Card Payments in Australia.

(c) The Card Issuer may outsource key parts of the CVM process for Third Party Digital Wallet transactions to a third party, but should ensure the third party meets the requirements in this section 1.2.

D.2.2 TOKENISATION

D2.2.1 Use of Tokenisation Services

(a) Tokenisation is not compulsory for transactions made using a Third Party Digital Wallet if the Third Party Digital Wallet includes an embedded secure element solution. In this case, it is up to the Card Issuer to decide if tokenisation services are appropriate for Third Party Digital Wallet transactions made using the Card Issuer's issued Cards.

(b) Tokenisation should be used for transactions made using a Third Party Digital Wallet if:

(i) mandated by applicable Card Scheme rules; or

(ii) the Third Party Digital Wallet does not include an embedded secure element solution.

D2.2.2 Selecting Tokenisation Services

(a) The Card Issuer is responsible for selecting token service provider/s, and may choose the tokenisation services of any TSP or supply its own tokenisation service, provided the chosen service conforms to the minimum standards prescribed by section 2.3.

(b) The Card Issuer may choose to use the tokenisation services of more than one TSP.

D2.2.3 Minimum standards

The Card Issuer should ensure that any TSP it engages to provide tokenisation services meets the minimum standards set out in EMVCo's *Payment Tokenisation Specification – Technical Framework*, version 1.0 (published March 2014).

D.2.3 PRIVACY – TREATMENT OF DATA GENERATED DURING TRANSACTIONS

D.2.3.1 Compliance with Privacy Act

All entities which collect, use and disclose Cardholder personal information in Australia are bound by their respective obligations under the Privacy Act.

D.2.3.2 Disclosure of Transaction Data to Card Issuers

It is advisable that the Card Issuer has effective arrangements in place to ensure that Digital Wallet Providers and, if applicable, other parties in a shared mobile payments network:

(a) have obtained Cardholders' informed consent to the disclosure of any authentication data and any geolocation data which may be collected by that Digital Wallet Provider or party in relation to a transaction effected using a Third Party Digital Wallet; and

(b) will disclose such information to the Card Issuer if it reasonably requests such information, from time to time, for the purposes of investigation and resolution of fraud, disputed and unauthorised transactions and Cardholder complaints.

The next page is Annexure E

Annexure E ISSUER AND ACQUIRER BEST PRACTICE GUIDELINES FOR CARD NOT PRESENT TRANSACTIONS [DELETED][85]

[Deleted]

END

[85] Deleted effective 1/1/20, version 010 r&p 002.19